Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2007

Date filed: February 7, 2008

Name of company covered by this certification:

Consolidated Telcom (Form 499 ID: 803199)
Consolidated Communications Networks, Inc. (Form 499 ID: 816876)

Name of signatory: Bryan W. Personne

Title of signatory: Chief Operating Officer & CPNI Compliance Officer

I, Bryan W. Personne, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules. *See attached accompanying statement of operating procedures.*

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

The company currently has no information with respect to the processes pretexters are using to attempt to access CPNI. At this time, we have not encountered known pretexting. Our protective measures against pretexters are outlined in the accompanying statement of operating procedures.

Signed: _____

Bryan W. Personne

Attachment: Accompanying Statement of Operating Procedures for Consolidated Telcom

Per the FCC CPNI rules [47 CFR §64.2009(e)] and as referenced in the attached signed certification, **Consolidated Telcom**, referred to as Company hereafter, hereby certifies that the Company, and its affiliates, is in compliance with the FCC CPNI rules and has outlined some of the important operating procedures utilized in order to ensure the Company's compliance in the protection of CPNI:

1. CPNI manual has been updated in order to account for all FCC CPNI rules, including the recent revisions, and has been adopted by our Company's board
2. CPNI Compliance officer has been designated to oversee all CPNI duties, training, and activity
    - Established an outbound marketing supervisory review process for the use of CPNI
    - Records are maintained for any marketing campaigns that utilize customers' CPNI for a minimum of one year
3. Employees have been trained on when they are, and are not, authorized to use or disclose CPNI
    - Disciplinary process has been defined and is in place for violations and/or breaches of CPNI
4. Carrier authentication requirements have been met
    - All customers are authenticated as being an authorized account contact before discussing CPNI (non-call detail or call detail) without utilizing readily available biographical or account information as defined by the FCC
    - Call detail is only released to customers during customer-initiated telephone contact if a password is provided. If the requesting customer does not provide a password and cannot answer the customer established security questions, only the following FCC approved methods are permitted for the release of the requested call detail:
        - Sending the requested detail to the address of record (only a physical or email address associated with that particular account that has been in our company files for at least 30 days)
        - Calling the customer back at the telephone of record (only disclosing if the customer was authenticated as being an authorized account contact)
        - Having customer come in to Company's office and provide a valid government issued photo ID
5. Notice to customer of account changes- Customers are notified when any of the following are changes or activity occurs on their account:
    - Password changed or created
    - security questions utilized for forgotten password
    - security questions revised
    - online account password changed or created
    - address of record
    - email address of record
6. Notice of unauthorized disclosure of CPNI- A notification process is in place in order to notify both law enforcement and customer(s) in the event of a CPNI breach within the timeline specified by the FCC
7. Opt-out method for approval of CPNI use for marketing campaigns is utilized.
    - Customers are notified bi-annually of their rights for the use of their CPNI in marketing campaigns
    - New customers are notified of the opt-out procedure as a part of the customer sign-up process
    - Billing system displays customer's opting status
    - Compliance officer retains CPNI notifications and opting records for at least two years
8. Additional protection measures are taken above and beyond the current FCC CPNI rules.
    - Company takes reasonable measures to discover and protect against activity that is indicative of pretexting
    - Company maintains security of all CPNI, including but not limited to:
        - Documents containing CPNI are shredded
        - Computer terminals are locked when employee is not at the station

Attachment: Accompanying Statement of Operating Procedures for Consolidated Communications Networks, Inc.

Per the FCC CPNI rules [47 CFR §64.2009(e)] and as referenced in the attached signed certification, **Consolidated Communications Networks, Inc**, referred to as Company hereafter, hereby certifies that the Company, and its affiliates, is in compliance with the FCC CPNI rules and has outlined some of the important operating procedures utilized in order to ensure the Company's compliance in the protection of CPNI:

1. CPNI manual has been updated in order to account for all FCC CPNI rules, including the recent revisions, and has been adopted by our Company's board
2. CPNI Compliance officer has been designated to oversee all CPNI duties, training, and activity
    - Established an outbound marketing supervisory review process for the use of CPNI
    - Records are maintained for any marketing campaigns that utilize customers' CPNI for a minimum of one year
3. Employees have been trained on when they are, and are not, authorized to use or disclose CPNI
    - Disciplinary process has been defined and is in place for violations and/or breaches of CPNI
4. Carrier authentication requirements have been met
    - All customers are authenticated as being an authorized account contact before discussing CPNI (non-call detail or call detail) without utilizing readily available biographical or account information as defined by the FCC
    - Call detail is only released to customers during customer-initiated telephone contact if a password is provided. If the requesting customer does not provide a password and cannot answer the customer established security questions, only the following FCC approved methods are permitted for the release of the requested call detail:
        - Sending the requested detail to the address of record (only a physical or email address associated with that particular account that has been in our company files for at least 30 days)
        - Calling the customer back at the telephone of record (only disclosing if the customer was authenticated as being an authorized account contact)
        - Having customer come in to Company's office and provide a valid government issued photo ID
5. Notice to customer of account changes- Customers are notified when any of the following are changes or activity occurs on their account:
    - Password changed or created
    - security questions utilized for forgotten password
    - security questions revised
    - online account password changed or created
    - address of record
    - email address of record
6. Notice of unauthorized disclosure of CPNI- A notification process is in place in order to notify both law enforcement and customer(s) in the event of a CPNI breach within the timeline specified by the FCC
7. Opt-out method for approval of CPNI use for marketing campaigns is utilized.
    - Customers are notified bi-annually of their rights for the use of their CPNI in marketing campaigns
    - New customers are notified of the opt-out procedure as a part of the customer sign-up process
    - Billing system displays customer's opting status
    - Compliance officer retains CPNI notifications and opting records for at least two years
8. Additional protection measures are taken above and beyond the current FCC CPNI rules.
    - Company takes reasonable measures to discover and protect against activity that is indicative of pretexting
    - Company maintains security of all CPNI, including but not limited to:
        - Documents containing CPNI are shredded
        - Computer terminals are locked when employee is not at the station